UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,342	04/12/2001	David John Craft	AUS920010088US1	3785

7590 01/04/2005

Joseph R. Burwell
Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, TX 78755-8022

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Offic Action Summary	**Applicati n N .** 09/833,342	**Applicant(s)** CRAFT ET AL.	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the c rrespondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3-13-2003*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-39 have been examined and are pending.

Information Disclosure Statement

The IDS submitted on 3/13/2003 has been considered by the examiner.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 20 recites the limitation "The method of claim 16" in line 1. There is insufficient antecedent basis for this limitation in the claim. The examiner assumes the applicant meant to state "The method of claim 19."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 and 6-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Easter et al (U.S. 5,559,889).

1. Claim 1: Easter et al disclose a method for configuring a semiconductor chip, the method comprising:

- Selecting a private cryptographic key (col 1, lines 48-59).
- Selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship (col 1, lines 48-59).
- Embedding the private cryptographic key and the public cryptographic key in a read-only memory on the semiconductor chip (col 5, lines 25-35).

As the public and private keys are different, they are not related by a cryptographic key pair relationship.

2. Claim 2: Easter et al disclose a method of clam 1 wherein the semiconductor chip provides interface processing at a client (col 4, lines 21-31).
3. Claim 3: Easter et al disclose a method of claim 1 wherein the embedded step further comprises the embedding of a serial number associated with the semiconductor chip (col 5, lines 25-35).
4. Claim 4: Easter et al disclose a method of claim 3 further comprising storing the public cryptographic key in a database in association with the serial number (col 5, last paragraph and col 6, lines 1-3).
5. Claim 6: Easter et al disclose an article of manufacture comprising:
   - A first read-only memory structure containing an embedded private cryptographic key (col 2, lines 35-41).
   - A second read-only memory structure containing an embedded public cryptographic key, wherein the public cryptographic key and the private

cryptographic key are not related by a cryptographic key pair relationship (col 2, lines 35-41).

The examiner has interpreted claim 6 as broadly as reasonable and determined that it is possible that the first and second memory structure can be the same structure.

6. Claim 7: Easter et al disclose an article of manufacture of claim 6 wherein the article of manufacture is a semiconductor chip (col 2, lines 35-41). An integrated circuit chip is inherently the same thing as a semi-conductor chip.
7. Claim 8: Easter et al disclose an article of manufacture of claim 7 wherein the semiconductor chip is capable of providing interface processing at a client (col 4, lines 21-31).

Claims 1, 5, 10, 13, and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold (U.S. 5,787,172).

1. Claim 1: Arnold discloses a method for configuring a semiconductor chip, the method comprising:
    - Selecting a private cryptographic key (col 2, lines 9-24).
    - Selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship (col 2, lines 9-24).
    - Embedding the private cryptographic key and the public cryptographic key in a read-only memory on the semiconductor chip (col 4, lines 1-17).

2. Claim 5: Arnold discloses a method of claim 1 wherein the private cryptographic key, and the public cryptographic key in the read-only memory are inaccessible to an input/output connection of the semiconductor chip (col 4, lines 36-40).

3. Claims 10, 13, and 16: Arnold discloses a method, apparatus and computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and server, comprising:

   - Generating a client message at the client (col 2, 2nd paragraph).
   - Retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client (col 2, 2nd paragraph and col 4, lines 14-18).
   - Encrypting the client message with the embedded server public key (col 2, 2nd paragraph).
   - Sending the client message to the server (col 2, 2nd paragraph).

   Claims 10, 13, and 16 differ in that claim 10 is a method and claim 16 is an apparatus with means for applying the methods of claim 10. Claim 16 is a computer program product in a computer-readable medium, where the computer program product comprises instructions for the methods of claim 10.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (U.S. 5,559,889) in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems – Part One" by Mark Merkow, June 22, 2000).

1. Claim 9: Easter et al failed to disclose an article of manufacture of claim 8 wherein the first read-only memory structure and the second read-only memory structure are contained within a cryptographic unit of a CPU chip. However, ecommerce.com discloses a single chip configuration which has a CPU, ROM, and a cryptographic unit ("Just What Are SmartCards?", line 1 and "Chip Families"). Ecommerce.com disclosed that a cryptographic co-processor could be added to the CPU for applications which require faster execution of cryptographic algorithms. Easter et al disclosed that their invention could be used in both a corporate and government environment. As such, though security is a major issue, so is the speed at which communication occur as the longer it takes for a client and server to communicate, the more costly the communication can become. Thus, one of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Easter et al's teachings with ecommerce.com's teaching of a single integrated circuit chip with built in read-only memory (to store the public and private keys) and a cryptographic co-processor unit to create a system that is both secure and allows for faster communication.

Claims 11, 14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. 5,787,172).

1. Claims 11, 14, and 17: Arnold discloses a method, apparatus, and computer program product of claims 10, 13, and 16 respectively, further comprising:
    - Retrieving client authentication data (col 3, 1st paragraph).
    - Retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client (col 2, lines 25-41).

    Arnold does not disclose:
    - Encrypting the client authentication data with the embedded client private key.
    - Storing the encrypted client authentication data in the client message.

    Arnold discloses that authentication can be done using just the public and private key of a client because if a client's message is encrypted with its private key, then only the valid client's public key can decrypt the message (col 2, lines 25-41). In this way the client is authenticated. Further, Arnold discloses that authentication can be done via an authentication data in the form of a certificate that is generated by a trusted authority (col 3, 1st paragraph). One of ordinary skill in the art at the time of the applicant invention would be motivated to combine these two authentication methods so that the authentication certificate/data is also encrypted with the client's private key as this would be a two-layered authentication and would naturally be more secure than just using one authentication method or the other.

Further, one of ordinary skill would recognize that storing the encrypted client authentication data in the client message would allow the recipient to verify that the message did in fact come from the real client. One thing to note in the example used by Arnold in column 2, lines 25-41 is that element A can be both a client and a server and likewise, element B can be both a client and a server.

Claims 12, 15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. 5,787,172) in view of Easter et al (U.S. 5,559,889).

1. Claims 12, 15, and 18: Arnold does not disclose a method of claim 11, apparatus of claim 14, and computer program product of claim 17, further comprising:
    - Retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client.
    - Storing a copy of the embedded client serial number in the client message.

    However, Easter et al disclose a serial number corresponding to the public/private key pair being stored in a read-only memory. Further, Easter et al disclose the use of the serial number to look up the public key of a client by a key manager (col 5, last paragraph and col 6, first paragraph). The key manager would look up the proper key when an entity transmits a serial number to it of a client whose public key the entity wish to discover. One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Arnold and Easter et al's teachings so that a client's serial number is also embedded in a client's message before sending the message. In this manner, when a server receives the message, it can also check to see that the serial number embedded in the client's message matches the client's serial number, thus making the communication more secure. In the case of the use of a key manager, it would also make sense to encrypt the serial number when transmitting to the key manager, as one would not normally want client's serial numbers read by just anyone.

Claims 19-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. 5,787,172).

1. Claims 19, 21, and 23: Arnold discloses a method, apparatus, and computer program product with instructions in a computer-readable medium for use in a data processing system for secure communication between a client and a server, further comprising:
    - Generating a server message at the server (col 2, lines 10-24).
    - Retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client (col 2, lines 10-24).
    - Encrypting the server message with the client public key (col 2, lines 10-24).
    - Sending the server message to the client (col 2, lines 10-24).

Arnold does not specifically disclose retrieving information that was requested by the client, but methods, apparatus, and computer program products in a computer-readable medium that does so is well known in the art at the time of the applicant's invention.

2. Claim 20, 22, and 24: Arnold discloses the method of claim 19, apparatus of claim 21, and computer program product of claim 23, further comprising:

   - Retrieving server authentication data (col 3, 1st paragraph).
   - Retrieving a server private key (col 2, lines 25-41).

   However, Arnold does not specifically disclose:

   - Encrypting the server authentication data with the server private key.
   - Storing the encrypted server authentication data in the server message.

   The examples used by Arnold in columns 2 and 3 can apply both to a client or server. As pointed out in the case of a client initiating a communication, combining the authentication methods in which an authentication data is used as well as a private key is used would make for a more secure communication means, so one of ordinary skill in the art at the time of the applicant's invention would be motivated to do so.

Claims 25-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. 5,787,172) in view of Easter et al (U.S. 5,559,889).

1. Claims 25, 27, and 29: Arnold discloses a method, apparatus, and computer program product in a computer-readable medium with instructions for use in a data processing system, comprising:

    - Receiving a client message from the client (col 2, 2nd paragraph).
    - Retrieving a server private key (col 2, 2nd paragraph).

    Arnold does not disclose:

    - Retrieving a client serial number from the decrypted client message.
    - Retrieving a client public key that is associatively stored with the client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client.

    However, as mentioned previously, the use of a serial number is known to Easter et al (col 5, last paragraph and col 6, lines 1-3). One of ordinary skill in the art would recognize the advantages of the client submitting its serial number along within its message to the server, as mentioned already, and it would be natural that the server would then decrypt the client's message and retrieve the client's serial number to further authenticate the client.

2. Claims 26, 28, and 30: Arnold discloses a method of claim 25, and apparatus of clam 27, and a computer program product of claim 29, further comprising:

    - Retrieving encrypted client authentication data from the client message (col 3, lines 1-25).

- Decrypting the client authentication data with the retrieved client public key (col 2, lines 25-42).
- Verifying the decrypted client authentication data (col 3, lines 1-25).

Claims 31-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. 5,787,172).

1. Claims 31, 34, and 37: Arnold discloses a method, apparatus with means for, and computer program product in a computer-readable medium with instructions for use in a data processing system comprising:
    - Retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client (col 2, lines 10-24).
    - Decrypting the server message with the embedded client private key (col 2, lines 10-24).

    Though Arnold does not specifically disclose receiving a server message from the server, methods, apparatus, and computer program products in a computer readable medium is already well known in the art at the time of the applicant's invention.
2. Claims 32, 35, and 38: Arnold discloses a method of claim 31, apparatus of claim 34, and computer program product of claim 37 further comprising:
    - Retrieving encrypted server authentication data from the server message (col 2, lines 25-41).
    - Retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client (col 2, lines 25-41).

- Decrypting the server authentication data with the embedded server public key (col 2, lines 25-41).
- Verifying the decrypted server authentication data (col 2, lines 25-41).

The server authentication data is the server's message itself as only a message that was encrypted using the server's private key could be decrypted properly using the server's public key.

3. Claims 33, 36, and 39: Arnold does not specifically disclose a method of claim 32, apparatus of claim 35, and computer program product of claim 38 further comprising:

- Retrieving requested information from the server message and
- In response to a determination that the encrypted server authentication data was verified, processing the requested information.

However, retrieving requested information from a server message is already well known at the time of the applicant's invention. Further, one of ordinary skill in the art at the time of the applicant's invention would naturally only process the requested information if the encrypted server authentication data was verified. Otherwise, there would be no point in having the server authenticated.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Rollins (U.S. 2002/0141588) discloses data encryption using public/private keys.
2. Gressel et al (U.S. 5,852,665) discloses sending and receiving messages that have been encrypted using public keys and decrypting the messages using private keys.
3. Khidekel et al (U.S. 6,636,975) discloses secure client and server communication.
4. Hellman et al (U.S. 4,200,770) discloses public and private key encryption/decryption methods.
5. Saito (U.S. 6,076,077) discloses a secure data management system in which data is encrypted.
6. Johnson et al (U.S. 5,604,800) discloses a secure communication and data access method through the use of an electronic key.
7. Sudia (U.S. 5,799,086) discloses public and private keys in ROM chips, where the public key is not related cryptographically to the private key.
8. "Data Encryption Standard (DES)" discloses Federal Information Processing Standards for cryptographic algorithms.
9. "Key Management for Large Scale End-to-End Encryption", by Witzke et al discloses asymmetric public key encryption.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100